.

CLASS POLYNOMIALS FOR NONHOLOMORPHIC MODULAR FUNCTIONS

JAN HENDRIK BRUINIER, KEN ONO, AND ANDREW V. SUTHERLAND

Abstract. We give algorithms for computing the *singular moduli* of suitable nonholomorphic modular functions $F(z)$. By combining the theory of *isogeny volcanoes* with a beautiful observation of Masser concerning the nonholomorphic Eisenstein series $E_2^*(z)$, we obtain CRT-based algorithms that compute the class polynomials $H_D(F;x)$, whose roots are the discriminant D singular moduli for $F(z)$. By applying these results to a specific weak Maass form $F_p(z)$, we obtain a CRT-based algorithm for computing *partition class polynomials*, a sequence of polynomials whose traces give the partition numbers $p(n)$. Under the GRH, the expected running time of this algorithm is $O(n^{5/2+o(1)})$. Key to these results is a fast CRT-based algorithm for computing the classical modular polynomial $\Phi_m(X,Y)$ that we obtain by extending the isogeny volcano approach previously developed for prime values of m.

1. Introduction and Statement of results

As usual, we let

$$j(z) := \frac{\left(1+240\sum_{n=1}^{\infty}\sum_{d|n} d^3q^n\right)^3}{q\prod_{n=1}^{\infty}(1-q^n)^{24}} = q^{-1}+744+196884q+21493760q^2+\cdots \tag{1.1}$$

be Klein's classical elliptic modular function on $\mathrm{SL}_2(\mathbb{Z})$ ($q := e^{2\pi iz}$ throughout). The values of $j(z)$ at imaginary quadratic arguments in the upper-half of the complex plane are known as *singular moduli*. Two examples are the Galois conjugates

$$j\left(\frac{1+\sqrt{-15}}{2}\right) = \frac{-191025-85995\sqrt{5}}{2} \quad \text{and} \quad j\left(\frac{1+\sqrt{-15}}{4}\right) = \frac{-191025+85995\sqrt{5}}{2}.$$

These numbers play an important role in algebraic number theory. Indeed, they are algebraic integers that generate ring class field extensions of imaginary quadratic fields, and they are the j-invariants of elliptic curves with complex multiplication [3, 9, 10, 11].

The problem of computing singular moduli has a long history that dates back to the works of Kronecker, and is highlighted by famous calculations by Berwick [2] and Weber [35]. Historically, these numbers have been difficult to compute. More recently, Gross and Zagier [21] determined the prime factorization of the absolute norm of suitable differences of singular moduli (further work in this direction has been carried out by Dorman [12, 13]), and Zagier [36] identified the algebraic traces of singular moduli as coefficients of half-integral weight modular forms.

The first author was supported by DFG grant BR-2163/2-2. The second author thanks the support of NSF grant DMS -1157289 and the Asa Griggs Candler Fund. The third author received support from NSF grant DMS-1115455.

Here we consider the problem of computing the minimal polynomials of singular moduli, the so-called Hilbert class polynomials. This problem has been the subject of much recent study. For example, Belding, Bröker, Enge, and Lauter [1], and the third author [33], have provided efficient methods of computation that are based on the theory of elliptic curves with complex multiplication (CM). The basic approach in that work is simple. One uses theoretical facts about elliptic curves with CM to quickly compute the reductions of these polynomials modulo a set of suitable primes p, and one then compiles these reductions via the Chinese Remainder Theorem (CRT) to obtain the exact polynomials. The primes p are chosen in a way that facilitates the computation, and in particular, they split completely in the ring class field $K_{\mathcal{O}}$ of the imaginary quadratic order $\mathcal{O}$ associated to the singular moduli whose minimal polynomial one wishes to compute. Under the Generalized Riemann Hypothesis (GRH), this algorithm computes the discriminant D Hilbert class polynomial with an expected running time of $\widetilde{O}(|D|)$.[1] In [6], the third author, together with Bröker and Lauter, further developed these ideas to compute modular polynomials Φ_ℓ using the theory of *isogeny volcanoes*.

We extend these results to the setting of nonholomorphic modular functions such as

$$\gamma(z) := \frac{E_4(z)}{6E_6(z)j(z)} \cdot E_2^*(z) - \frac{7j(z) - 6912}{6j(z)(j(z) - 1728)}, \tag{1.2}$$

where

$$E_2^*(z) := 1 - \frac{3}{\pi \mathrm{Im}(z)} - 24 \sum_{n=1}^{\infty} \sum_{d|n} dq^n \tag{1.3}$$

is the weight 2 nonholomorphic modular Eisenstein series, and where

$$E_4(z) := 1 + 240 \sum_{n=1}^{\infty} \sum_{d|n} d^3 q^n \quad \text{and} \quad E_6(z) := 1 - 504 \sum_{n=1}^{\infty} \sum_{d|n} d^5 q^n$$

are the usual weight 4 and weight 6 modular Eisenstein series.

Remark. The function $\gamma(z)$ plays an important role in this paper. We shall make use of an observation of Masser [27] which gives a description of its singular moduli in terms of the coefficients of certain representations of the classical modular polynomials.

We first recall the setting of Heegner points on modular curves (see [20]). Let $N > 1$, and let $D < 0$ be a quadratic discriminant coprime to N. The group $\Gamma_0(N)$ acts on the discriminant D positive definite integral binary quadratic forms

$$Q(X, Y) = [a, b, c] := aX^2 + bXY + cY^2$$

with $N \mid a$. This action preserves $b \pmod{2N}$. Therefore, if $\beta^2 \equiv D \pmod{4N}$, then it is natural to consider $\mathcal{Q}_{N,D,\beta}$, the set of those discriminant D forms $Q = [a, b, c]$ for which $0 < a \equiv 0 \pmod{N}$ and $b \equiv \beta \pmod{2N}$, and we may also consider the subset $\mathcal{Q}_{N,D,\beta}^{\mathrm{prim}}$ obtained by restricting to primitive forms. The number of $\Gamma_0(N)$ equivalence classes in $\mathcal{Q}_{N,D,\beta}$ is the Hurwitz-Kronecker class number $H(D)$, and the natural map defines a bijection

$$\mathcal{Q}_{N,D,\beta}/\Gamma_0(N) \longrightarrow \mathcal{Q}_D/\mathrm{SL}_2(\mathbb{Z}),$$

[1] We use the "soft" asymptotic notation $\widetilde{O}(n)$ to denote bounds of the form $O(n \log^c n)$.

where $\mathcal{Q}_D$ is the set of discriminant D positive definite integral binary quadratic forms (see the proposition on p. 505 of [20]). This bijection also holds when restricting to primitive forms, in which case the number of $\Gamma_0(N)$ equivalence classes in $\mathcal{Q}^{\text{prim}}_{N,D,\beta}$, and the number of $\mathrm{SL}_2(\mathbb{Z})$ equivalence classes in $\mathcal{Q}^{\text{prim}}_D$, is given by the class number $h(D)$.

For modular functions $F(z)$ on $\mathrm{SL}_2(\mathbb{Z})$, our goal is to calculate the *class polynomial*

$$H_D(F;x) := \prod_{Q \in \mathcal{Q}_D^{\text{prim}}/\mathrm{SL}_2(\mathbb{Z})} \big(x - F(\alpha_Q)\big), \tag{1.4}$$

where $\alpha_Q \in \mathbb{H}$ is a root of $Q(x,1) = 0$. For modular functions $F(z)$ on $\Gamma_0(N)$ and discriminants $D < 0$ coprime to N, our goal is to calculate the *class polynomial*

$$H_{D,\beta}(F;x) := \prod_{Q \in \mathcal{Q}_{N,D,\beta}^{\text{prim}}/\Gamma_0(N)} \big(x - F(\alpha_Q)\big). \tag{1.5}$$

We first consider the special case of the $\mathrm{SL}_2(\mathbb{Z})$ nonholomorphic modular function $\gamma(z)$, defined by (1.2), and we compute the $\mathbb{Q}$-rational polynomials $H_D(\gamma;x)$.

Theorem 1.1. *For discriminants $D < -4$ that are not of the form $D = -3d^2$, Algorithm 1 (see §3.1) computes $H_D(\gamma;x)$. Under the GRH, its expected running time is $\widetilde{O}(|D|^{7/2})$ and it uses $\widetilde{O}(|D|^2)$ space.*

Remark. The discussion on p. 118 of [27], makes it clear how to modify Algorithm 1 to handle discriminants of the form $D = -3d^2$. We expect that the bound on its expected running time can be improved to $\widetilde{O}(|D|^{5/2})$ using tighter bounds on the size of the coefficients of $H_D(\gamma;x)$.

A key building block of Algorithm 1 is a new algorithm to compute the classical modular polynomial $\Phi_m(X,Y)$, which parameterizes pairs of elliptic curves related by a cyclic isogeny of degree m. Here we extend the iosgeny volcano approach that was introduced in [6] to compute Φ_m for prime m so that we can now efficiently handle all values of m. The result is Algorithm 1.1 (see §3.1), which, under the GRH, computes Φ_m in $\tilde{O}(m^3)$ time. For suitable primes p it can compute Φ_m modulo p in $\tilde{O}(m^2)$ time (and space), which is crucial to the efficient implementation of Algorithm 1.

Example. We have used Algorithm 1 to compute $H_D(\gamma,x)$ for $D > -20000$. Some small examples are listed below.

D	$H_D(\gamma, x)$
-3	$x - \frac{23}{2^{11}\cdot 3^3}$
-4	x
-7	$x - \frac{181}{3^6\cdot 5^3\cdot 7}$
-8	$x + \frac{61}{2^6\cdot 5^3\cdot 7^2}$
-11	$x - \frac{289}{2^{14}\cdot 7^2\cdot 11}$
-12	$x + \frac{67}{2^3\cdot 3^3\cdot 5^3\cdot 11^2}$
-15	$x^2 + \frac{313}{3^4\cdot 5\cdot 11^3}\cdot x - \frac{1045769}{3^8\cdot 5^3\cdot 7^4\cdot 11^5}$
-16	$x + \frac{179}{3^6\cdot 7^2\cdot 11^3}$
-19	$x - \frac{275}{2^{14}\cdot 3^6\cdot 19}$
-20	$x^2 - \frac{43925}{2^6\cdot 11^3\cdot 19^2}\cdot x - \frac{2307859}{2^{18}\cdot 5^3\cdot 11^5\cdot 19^2}$
-23	$x^3 + \frac{8123835989}{5^3\cdot 7^2\cdot 11^3\cdot 17^3\cdot 19^2\cdot 23}\cdot x^2 + \frac{6062055706222}{5^6\cdot 7^4\cdot 11^4\cdot 17^3\cdot 19^2\cdot 23}\cdot x - \frac{346923509992369}{5^6\cdot 7^4\cdot 11^4\cdot 17^3\cdot 19^2\cdot 23}$

We extend Algorithm 1 to compute class polynomials for a large class of nonholomorphic modular functions. This class includes, for example, the $\mathrm{SL}_2(\mathbb{Z})$-function

$$K(z) := 288 \cdot \frac{E_2^*(z)E_4(z)E_6(z) + 3E_4(z)^3 + 2E_6(z)}{E_4(z)^3 - E_6(z)^2}$$

considered by Zagier (see §9 of [36]) in his famous paper on traces of singular moduli. More generally, it includes suitable modular functions $F(z)$ of the form

$$F(z) := \partial_{-2} \circ \partial_{-4} \cdots \partial_{2-2k}(\mathfrak{F}),$$

where $\mathfrak{F}(z)$ is a weight $2-2k$ weakly holomorphic modular form on $\Gamma_0(N)$ whose Fourier expansions at cusps are algebraic. Here the differential operator ∂_h, which maps weight h modular forms to weight $h+2$ modular forms, is defined by

$$\partial_h := \frac{1}{2\pi i}\cdot\frac{\partial}{\partial z} - \frac{h}{4\pi \mathrm{Im}(z)}. \tag{1.6}$$

We consider a specific class of such modular functions. Let $\mathcal{O}$ be the imaginary quadratic order with discriminant D, ring class field $K_{\mathcal{O}}$, and fraction field $K = \mathbb{Q}(\sqrt{D})$. Let c_1 and c_2 denote fixed positive integers. Let $F(z)$ be a modular function (i.e. weight 0) for $\Gamma_0(N)$ that

can be written in the form

$$F(z) = \sum A_n(z)\gamma(z)^n,$$

where each $A_n \in \mathbb{Q}(j)$ is a rational function of $j(z)$. The function $F(z)$ is said to be **good** for a discriminant $D < 0$ coprime to N if it satisfies the following:

(1) Each $A_n(\alpha_Q)$ lies in $K_{\mathcal{O}}$ for all $Q \in \mathcal{Q}_D^{\text{prim}}/\mathrm{SL}_2(\mathbb{Z})$.
(2) The polynomial $c_1|D|^{c_2 h} H_D(F; x)$ has integer coefficients.

Remark. The class of good modular functions includes many nonholomorphic modular functions, such as $\gamma(z)$, and it includes meromorphic modular functions which may have poles in the upper half plane (poles at CM points are excluded by condition (1)).

For good modular functions, we obtain the following general result.

Theorem 1.2. *For discriminants $D < -4$ not of the form $D = -3d^2$, Algorithm 2 (see §3.2) computes class polynomials for good modular functions $F(z)$. Under the GRH, its expected running time is $\widetilde{O}(|D|^{5/2})$, and it uses $\widetilde{O}(|D|^2)$ space.*

In fact, Algorithm 2 can be readily adapted to treat modular functions of the form $F(z) = \sum A_n(z)\gamma(z)^n$ where the coefficient functions $A_n(z)$ do not necessarily lie in $\mathbb{Q}(j)$, using the techniques developed by Enge and the third author in [16]. As an example, we apply Algorithm 2 to obtain a CRT-based algorithm for computing the "partition polynomials" defined by the first two authors in [8]. These are essentially the class polynomials of the $\Gamma_0(6)$ nonholomorphic modular function

$$F_p(z) := -\partial_{-2}(P(z)) = \left(1 - \frac{1}{2\pi \mathrm{Im}(z)}\right) q^{-1} + \frac{5}{\pi \mathrm{Im}(z)} + \left(29 + \frac{29}{2\pi \mathrm{Im}(z)}\right) q + \ldots, \tag{1.7}$$

where $P(z)$ is the weight -2 weakly holomorphic modular form

$$P(z) := \frac{1}{2} \cdot \frac{E_2(z) - 2E_2(2z) - 3E_2(3z) + 6E_2(6z)}{\eta(z)^2\eta(2z)^2\eta(3z)^2\eta(6z)^2} = q^{-1} - 10 - 29q + \ldots.$$

These polynomials are defined as

$$H_n^{\text{part}}(x) := \prod_{Q \in \mathcal{Q}_{6,1-24n,1}} (x - P(\alpha_Q)). \tag{1.8}$$

In contrast with (1.4) and (1.5), we stress that the roots of these polynomials include singular moduli for imprimitive forms (if any). The interest in these polynomials arises from the fact that (see Theorem 1.1 of [8])

$$H_n^{\text{part}}(x) = x^{h(1-24n)} - (24n-1)p(n)x^{h(1-24n)-1} + \ldots, \tag{1.9}$$

where $p(n)$ is the usual partition function. Since the roots $P(\alpha_Q)$ are algebraic numbers that lie in the usual discriminant $1 - 24n$ ring class field, we have the following finite algebraic formula

$$p(n) = \frac{1}{24n-1} \sum_{Q \in \mathcal{Q}_{6,1-24n,1}} P(\alpha_Q).$$

Remark. By the work of the first two authors [8], combined with recent results by Larson and Rolen [26], it is known that each $(24n-1)P(\alpha_Q)$ is an algebraic integer.

As a consequence of Theorem 1.2, we obtain the following result.

Theorem 1.3. *For all positive integers n, Algorithm 3 (see §3.3) computes $H_n^{\mathrm{part}}(x)$. Under the GRH, its expected running time is $\widetilde{O}(n^{5/2})$ and it uses $\widetilde{O}(n^2)$ space.*

Remark. For the simpler task of computing individual values of $p(n)$, an efficient implementation of Rademacher's formula such as the one given in [23] is both asymptotically and practically faster than Algorithm 3.

Example. We have used Algorithm 3 to compute $H_n^{\mathrm{part}}(x)$ for $n \le 750$. Some small examples are listed below.

n	$(24n-1)p(n)$	$H_n^{\mathrm{part}}(x)$
1	23	$x^3 - 23x^2 + \frac{3592}{23}x - 419$
2	94	$x^5 - 94x^4 + \frac{169659}{47}x^3 - 65838x^2 + \frac{1092873176}{47^2}x + \frac{1454023}{47}$
3	213	$x^7 - 213x^6 + \frac{1312544}{71}x^5 - 723721x^4 + \frac{44648582886}{71^2}x^3 + \frac{9188934683}{71}x^2 + \frac{166629520876208}{71^3}x + \frac{2791651635293}{71^2}$
4	475	$x^8 - 475x^7 + \frac{9032603}{95}x^6 - 9455070x^5 + \frac{3949512899743}{95^2}x^4 - \frac{97215753021}{19}x^3 + \frac{9776785708507683}{95^3}x^2 - \frac{53144327916296}{19^2}x - \frac{134884469547631}{5^4\cdot 19}$

This paper is organized as follows. In §2 we recall essential facts about elliptic curves with complex multiplication, and singular moduli for modular forms and certain nonholomorphic modular functions. In §3 we use these results to derive our algorithms. In §4 we conclude with a detailed example of the execution of Algorithm 3 for $n = 1$ and $n = 24$.

2. Nuts and bolts

We begin with some preliminaries on elliptic curves with complex multiplication and singular moduli for suitable modular functions.

2.1. **Elliptic curves with complex multiplication.** We recall some standard facts from the theory of complex multiplication, referring to [9, 25, 30] for proofs and further background. Let $\mathcal{O}$ be an imaginary quadratic order, identified by its discriminant D. The j-invariant of the lattice $\mathcal{O}$ is an algebraic integer whose minimal polynomial is the *Hilbert class polynomial* H_D. If $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal (including $\mathfrak{a} = \mathcal{O}$), then the torus $\mathbb{C}/\mathfrak{a}$ corresponds to an elliptic curve $E/\mathbb{C}$ with *complex multiplication* (CM) by $\mathcal{O}$, meaning that its endomorphism ring $\mathrm{End}(E)$ is isomorphic to $\mathcal{O}$, and every such curve arises in this fashion. Equivalent ideals

yield isomorphic elliptic curves, and this gives a bijection between the ideal class group $\mathrm{cl}(\mathcal{O})$ and the set

$$\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) := \{j(E/\mathbb{C})\colon \mathrm{End}(E) \cong \mathcal{O}\}, \tag{2.1}$$

the j-invariants of the elliptic curves defined over $\mathbb{C}$ with CM by $\mathcal{O}$. We then have

$$H_D(x) := \prod_{j_i \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})} (x - j_i) = H_D(j; x). \tag{2.2}$$

The splitting field of H_D over $K = \mathbb{Q}(\sqrt{D})$ is the *ring class field* $K_{\mathcal{O}}$. It is an abelian extension whose Galois group is isomorphic to $\mathrm{cl}(\mathcal{O})$, via the Artin map.

This isomorphism can be made explicit via isogenies. Let $E/\mathbb{C}$ be an elliptic curve with CM by $\mathcal{O}$ and let $\mathfrak{a}$ be an invertible $\mathcal{O}$-ideal. There is a uniquely determined separable isogeny whose kernel is the subgroup of points annihilated by every endomorphism in $\mathfrak{a} \subset \mathcal{O} \hookrightarrow \mathrm{End}(E)$. The image of this isogeny is an elliptic curve that also has CM by $\mathcal{O}$, and this defines an action of the ideal group of $\mathcal{O}$ on the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. Principal ideals act trivially, and the induced action of the class group is regular. Thus $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is a principal homogeneous space, a *torsor*, for the finite abelian group $\mathrm{cl}(\mathcal{O})$.

If p is a (rational) prime that splits completely in $K_{\mathcal{O}}$, equivalently, for $p > 3$, a prime satisfying the *norm equation*

$$4p = t^2 - v^2 D \tag{2.3}$$

for some nonzero integers t and v, then H_D splits completely in $\mathbb{F}_p[x]$ and its roots form the set

$$\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p) := \{j(E/\mathbb{F}_p)\colon \mathrm{End}(E) \cong \mathcal{O}\}, \tag{2.4}$$

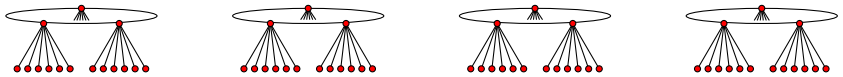
Conversely, every ordinary (not supersingular) elliptic curve $E/\mathbb{F}_p$ has CM by some imaginary quadratic order $\mathcal{O}$ in which the Frobenius endomorphism corresponds to an element of norm p and trace t.

2.2. **Modular polynomials via isogeny volcanoes.** For each positive integer m, the classical modular polynomial Φ_m is the minimal polynomial of the function $j(mz)$ over the field $\mathbb{C}(j)$. As a polynomial in two variables, $\Phi_m \in \mathbb{Z}[X, Y]$ is symmetric in X and Y. If E/k is an elliptic curve and N is prime to the characteristic of k, then the roots of $\Phi_m(j(E), Y)$ are precisely the j-invariants of the elliptic curves that are related to E by a cyclic m-isogeny; see [25] for these and other properties of Φ_m.

For distinct primes ℓ and p, we define the *graph of ℓ-isogenies* $G_\ell(\mathbb{F}_p)$, with vertex set $\mathbb{F}_p$ and edges (j_1, j_2) present if and only if $\Phi_\ell(j_1, j_2) = 0$. Ignoring the connected components of 0 and 1728, the ordinary components of $G_\ell(\mathbb{F}_p)$ are *ℓ-volcanoes* [17, 24], a term we take to include cycles as a special case; see [34] for further details on isogeny volcanoes. In this paper we focus on ℓ-volcanoes of a special form, for which we can compute $\Phi_\ell \bmod p$ in a particularly efficient way, using [6, Alg. 2.1].

Let $\mathcal{O}$ be an order in an imaginary quadratic field K with maximal order $\mathcal{O}_K$, and let ℓ be an odd prime not dividing $[\mathcal{O}_K : \mathcal{O}]$. Assume $D = \mathrm{disc}(\mathcal{O}) < -4$. Suppose p is a prime of the form $4p = t^2 - \ell^2 v^2 D$ with $p \equiv 1 \bmod \ell$ and $\ell \nmid v$; equivalently, p splits completely in the ray class field of conductor ℓ for $\mathcal{O}$ and does not split completely in the ring class field of the order

with index ℓ^2 in $\mathcal{O}$. Then the components of $G_\ell(\mathbb{F}_p)$ that intersect $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ are isomorphic ℓ-volcanoes with two levels: the *surface*, whose vertices lie in $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$, and the *floor*, whose vertices lie in $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_p)$, where $\mathcal{O}'$ is the order of index ℓ in $\mathcal{O}$. Each vertex on the surface is connected to $1+\left(\frac{D}{\ell}\right) = 0, 1$ or 2 *siblings* on the surface, and $\ell - \left(\frac{D}{\ell}\right)$ *children* on the floor. An example with $\ell = 7$ is shown below:



Provided $h(\mathcal{O}) \geq \ell + 2$, this set of ℓ-volcanoes contains enough information to completely determine $\Phi_\ell \bmod p$. This is the basis of the algorithm in [6, Alg. 2.1] to compute $\Phi_\ell \bmod p$, which we make use of here. Selecting a sufficiently large set of such primes p allows one to compute Φ_ℓ over $\mathbb{Z}$ (via the CRT), or modulo an arbitrary integer M (via the explicit CRT). Our requirements for the order $\mathcal{O}$ and the primes p are summarized in the definition below.

Definition 2.1. Let $\ell > 2$ be prime, and let $c > 1$ be an absolute constant independent of ℓ. An imaginary quadratic order $\mathcal{O}$ is said to be *suitable* for ℓ if $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ and $\ell + 2 \leq h(\mathcal{O}) \leq c\ell$. A prime p is then said to be *suitable* for ℓ and $\mathcal{O}$ if $p \equiv 1 \bmod \ell$ and $4p = t^2 - \ell^2 v^2 \operatorname{disc}(\mathcal{O})$, for some $t, v \in \mathbb{Z}$ with $\ell \nmid v$.

The definition of suitability above is weaker than that used in [6], but this only impacts logarithmic factors in the running time that are hidden by our soft asymptotic notation.

2.3. **Selecting primes with the GRH.** In order to apply the isogeny volcano method to compute Φ_ℓ (or the polynomials $H_D(F;x)$ we wish to compute), we need a sufficiently large set S of suitable primes p. We deem S to be sufficiently large whenever $\sum_{p\in S} \log p \geq B + \log 2$, where B is an upper bound on the logarithmic height of the integer coefficients that we wish to compute with the CRT.[2] For $\Phi_\ell(X,Y) = \sum_{i,j} a_{ij} X^i Y^j$, we may bound $\mathrm{ht}(\Phi_\ell) := \log \max_{i,j} |a_{ij}|$ using

$$\mathrm{ht}(\Phi_\ell) \leq 6\ell \log \ell + 18\ell, \tag{2.5}$$

as proved in [7].

Heuristically (and in practice), it is easy to construct the set S. Given an order $\mathcal{O}$ of discriminant D suitable for ℓ, we fix $v = 2$ if $D \equiv 1 \bmod 8$ and $v = 1$ otherwise, and for increasing $t \equiv 2 \bmod \ell$ of correct parity we test whether $p = (t^2 - v^2\ell^2 D)/4$ is prime. We add each such prime to S, and stop when S is sufficiently large.

Unfortunately, we cannot prove that this method will find *any* primes, even under the GRH. Instead, we use Algorithm 6.2 in [6], which picks an upper bound x and generates random integers t and v in suitable intervals to obtain candidate primes $p = (t^2 - v^2\ell^2 D)/4 \leq x$ that are then tested for primality. The algorithm periodically increases x, so its expected running time is $O(B^{1+\epsilon})$, even without the GRH.

Under the GRH, there are effective constants $c_1, c_2 > 0$ such that $x \geq c_1 \ell^6 \log^4 \ell$ guarantees at least $c_2 \ell^3 \log^3 \ell$ suitable primes less than x, by [6, Thm. 4.4]. Asymptotically, this is far more than the $O(\ell)$ primes we need to compute Φ_ℓ. We note that S contains $O(B/\log B)$ primes (unconditionally), and under the GRH we have $\log p = O(\log B + \log \ell)$ for all $p \in S$.

[2] When the coefficients are rational numbers that are not integers, we first clear denominators.

2.4. **Modular singular moduli.** The results from the previous section can be cast in terms of the CM values of the j-function. Indeed, we have the following classical theorem (for example, see [3, 9]) which summarizes some of the most important properties of singular moduli for Klein's j-function.

Theorem 2.2. *Suppose that $Q = ax^2 + bxy + cy^2$ is a primitive positive definite binary quadratic form with discriminant $D = b^2 - 4ac < 0$, and let $\alpha_Q \in \mathbb{H}$ be the point for which $Q(\alpha_Q, 1) = 0$. Then the following are true:*

(1) The singular modulus $j(\alpha_Q)$ is an algebraic integer whose minimal polynomial has degree equal to the class number $h(D)$.
(2) The Galois orbit of $j(\alpha_Q)$ consists of the $j(z)$-singular moduli associated to the $h(D)$ equivalence classes in $\mathcal{Q}_D^{\text{prim}}/\mathrm{SL}_2(\mathbb{Z})$.
(3) If $K = \mathbb{Q}(\sqrt{D})$, then the discriminant D singular moduli are conjugate over K. Moreover, $K(j(\alpha_Q))$ is the ring class field of the quadratic order of discriminant D; in the case that D is a fundamental discriminant, $K(j(\alpha_Q))$ is the Hilbert class field of K.

Theorem 2.2 and the properties of the weight 2 nonholomorphic Eisenstein series $E_2^*(z)$ at CM points shall play a central role in the construction of the algorithms described in the next section. To this end, we make use of the special nonholomorphic function $\gamma(z)$ defined in (1.2).

Masser nicely observed that the singular moduli for $\gamma(z)$ can be computed using the singular moduli for $j(z)$ and certain expressions for modular polynomials. Here we make this precise for discriminants $D < -4$ that are not of the form $D = -3d^2$.

Remark. Masser explains how to handle discriminants $D = -3d^2$; see p. 118 of [27].

To state his observation, we let $\mathcal{O}$ be the imaginary quadratic order of discriminant D, and let $\{Q_1, \dots, Q_h\}$ be a set of representatives for $\mathcal{Q}_D^{\text{prim}}/\mathrm{SL}_2(\mathbb{Z}) \simeq \mathrm{cl}(\mathcal{O})$, where $h = h(D)$ is the class number. To simplify notation, we use Φ_D to denote the classical modular polynomial $\Phi_{|D|}(X, Y)$. For any $Q = Q_i$ we may write Φ_D in the form

$$\Phi_D(X, Y) = \sum_{0 \le \mu, \nu \le n} \beta_{\mu,\nu} \big(X - j(\alpha_Q)\big)^{\mu} \big(Y - j(\alpha_Q)\big)^{\nu}, \tag{2.6}$$

where $n = \psi(|D|)$ is determined by the Dedekind ψ-function

$$\psi(m) := m \prod_{p \mid m} (1 + p^{-1}), \tag{2.7}$$

which satisfies $\psi(m) = O(m \log\log m)$; see [32]. The coefficients $\beta_{\mu,\nu} = \beta_{\mu,\nu}(\alpha_Q)$ are algebraic integers that lie in the ring class field $K_{\mathcal{O}}$, and we have $\beta_{\mu,\nu} = \beta_{\nu,\mu}$ (by the symmetry of Φ_D). Masser [27, p. 118] gives the following formula for $\gamma(\alpha_Q)$.

Lemma 2.3. *Assuming the notation and hypotheses above, we have*

$$\gamma(\alpha_Q) = \frac{2\beta_{0,2}(\alpha_Q) - \beta_{1,1}(\alpha_Q)}{\beta_{0,1}(\alpha_Q)}. \tag{2.8}$$

Two remarks.
1) Masser proves (see [27, Lem. A2]) that $\beta_{0,1}(\alpha_Q)$ is nonzero.
2) From (2.6), one finds that

$$\begin{aligned}\beta_{0,1}(\alpha_Q) &= [Y]\Phi_D\big(j(\alpha_Q), Y + j(\alpha_Q)\big),\\ \beta_{1,1}(\alpha_Q) &= [Y]\Phi'_D\big(j(\alpha_Q), Y + j(\alpha_Q)\big),\\ \beta_{0,2}(\alpha_Q) &= [Y^2]\Phi_D\big(j(\alpha_Q), Y + j(\alpha_Q)\big),\end{aligned} \tag{2.9}$$

where $\Phi'_D(X,Y) = \frac{\partial}{\partial X}\Phi_D(X,Y)$, and for any polynomial $f(Y)$, the notation $[Y^k]f(Y)$ indicates the coefficient of Y^k in $f(Y)$.

3. The Algorithms

Here we apply and extend the results in §2 to derive our algorithms.

3.1. **Algorithm 1.** We now give an algorithm to compute the class polynomial $H_D(\gamma; x)$, where $\gamma(z)$ is the nonholomorphic modular function defined in (1.2) and D is an imaginary quadratic discriminant. In order to simplify the exposition as above, we shall assume $D < -4$ and that D is not of the form $D = -3d^2$; these *special* discriminants are in principle no more difficult to handle than the general case, but the details are more involved; see [27, p. 118].[3]

To make use of Lemma 2.3, we need to compute the singular moduli $j(\alpha_Q)$. These shall be obtained as the roots of the Hilbert class polynomial $H_D(x)$. Thus if we know Φ_D and H_D, then we can apply Lemma 2.3 to compute

$$H_D(\gamma; x) = \prod_{Q \in \mathcal{Q}_D^{\mathrm{prim}}/\mathrm{SL}_2(\mathbb{Z})} \big(x - \gamma(\alpha_Q)\big).$$

Using algorithms for fast multipoint polynomial evaluation and fast integer arithmetic (see [18], for example), this yields an algorithm that computes $H_D(\gamma; x)$ in $\widetilde{O}(|D|^3)$ expected time using $\widetilde{O}(|D|^3)$ space, under the GRH. However, this approach is quite memory intensive and quickly becomes impractical, even for moderate values of D. As an alternative, we give a CRT-based algorithm that uses $\widetilde{O}(|D|^{7/2})$ expected time and $\widetilde{O}(|D|^2)$ space, under the GRH.[4]

It is clear from equations (2.6) and (2.8) that the coefficients of $H_D(\gamma; x)$ lie in $\mathbb{Q}$; indeed, the coefficients of Φ_D are integers, as are the elementary symmetric functions of the $j(\alpha_Q)$, which are the coefficients of the Hilbert class polynomial $H_D(x)$. If we let

$$\delta := \prod_{Q \in \mathcal{Q}_D^{\mathrm{prim}}/\mathrm{SL}_2(\mathbb{Z})} \beta_{0,1}(\alpha_Q), \tag{3.1}$$

then $\delta \in \mathbb{Z}$ is divisible by the denominator of every coefficient of $H_D(\gamma; x)$ and $\delta H_D(\gamma; x) \in \mathbb{Z}[x]$. We now present the algorithm.

Algorithm 1
Input: An imaginary quadratic discriminant D that is not special.

[3] We note that the discriminants $D = 1 - 24n$ needed to compute $H_n^{\mathrm{part}}(x)$ are not special.

[4] As remarked in the introduction, we expect this running time can be improved, possibly to $\widetilde{O}(|D|^{5/2})$, by obtaining tighter bounds on the coefficients of $H_D(\gamma; x)$.

Output: The polynomial $H_D(\gamma;x) \in \mathbb{Q}[x]$.

1. Pick an order $\mathcal{O}$ suitable for $|D|$, and a set S of primes suitable for $|D|$ and $\mathcal{O}$ (see Def. 3.2), using the bound $B_\gamma(D)$ given in (3.3) below.
2. Compute the Hilbert class polynomial $H_D \in \mathbb{Z}[x]$ using [33, Alg. 2].
3. For each prime $p \in S$:
   a. Compute $\Phi = \Phi_D \bmod p$ using Algorithm 1.1 below.
   b. Compute $\Phi' = \frac{\partial}{\partial X}\Phi_D(X,Y) \bmod p$.
   c. Compute the roots $j_1, \dots, j_h \in \mathbb{F}_p$ of $H_D \bmod p$.
   d. Compute $\phi_k(Y) = \Phi(j_k, Y)$ and $\phi_k'(Y) = \Phi'(j_k, Y)$ for all j_k using [18, Alg. 10.7].
   e. For each j_k, compute $\beta_{0,1}, \beta_{1,1}$, and $\beta_{0,2}$ using ϕ_k and ϕ_k' via (2.9), and then compute $\gamma_k = (2\beta_{0,2} - \beta_{1,1})/\beta_{0,1}$.
   f. Compute $\delta = \prod_k \beta_{0,1}$ and $f(x) = \delta \prod_k (x - \gamma_k)$.
   g. Save $f(x) \bmod p$ and $\delta \bmod p$.
4. Use the CRT to recover $f(x) = \delta H_D(\gamma;x) \in \mathbb{Z}[x]$ and $\delta \in \mathbb{Z}$.
5. Output $H_D(\gamma;x) = \frac{1}{\delta} f(x) \in \mathbb{Q}[x]$.

Let $B_\Phi(D)$ denote an upper bound on $\mathrm{ht}(\Phi_D)$; when $|D|$ is prime we may use the bound $B_\Phi(D) = 6|D| + 18|D|\log|D|$ from (2.5), and otherwise we may derive such a bound by expressing Φ_D in terms of modular polynomials of prime level, as in [9, Thm. 13.14]. We use

$$M(D) := \log\bigl(\exp(\pi\sqrt{|D|}) + 2114.567\bigr) \tag{3.2}$$

to bound $\log|j(\alpha_Q)|$, for any $Q \in \mathcal{Q}_D^{\mathrm{prim}}$; see [14, p. 1094], for example.

We now define

$$B_\gamma(D) := \bigl(h(D)+1\bigr)\Bigl(4\log\bigl(\psi(|D|)+1\bigr) + 2\psi(|D|)M(D) + B_\Phi(D) + 2\Bigr). \tag{3.3}$$

Lemma 3.1. *Let D be an imaginary quadratic discriminant that is not special. Then we have the bounds $\delta \le B_\gamma(D)$ and $\mathrm{ht}(\delta H_D(\gamma;x)) \le B_\gamma(D)$, and $\delta = \widetilde{O}(|D|^{3/2})$.*

Proof. For any $Q \in \mathcal{Q}_D^{\mathrm{prim}}$, each coefficient c of the univariate polynomial $\phi(Y) = \Phi_D(j(\alpha_Q), Y)$ is a polynomial of degree $\psi(|D|)$ in $j(\alpha_Q)$ with coefficients bounded by $\mathrm{ht}(\Phi_D) \le B_\Phi(D)$. It follows that

$$\mathrm{ht}(\phi) \le \psi(|D|)M(D) + B_\Phi(D) + \log(\psi(|D|)+1). \tag{3.4}$$

From (2.9), we know that $\beta_{0,1}(\alpha_Q)$ is the linear coefficient of $\phi(Y + j(\alpha_Q))$, where $\phi(Y)$ has degree $\psi(|D|)$, and this implies

$$\log|\beta_{0,1}(\alpha_Q)| \le 2\log(\psi(|D|+1) + \mathrm{ht}(\phi) + \psi(|D|)M \tag{3.5}$$

for all $Q \in \mathcal{Q}_D^{\mathrm{prim}}$. Substituting (3.4) into 3.5 and applying the bound to each of the $h(D)$ factors in the product $\delta = \prod_Q \beta_{0,1}(\alpha_Q)$ yields

$$\log|\delta| \le h(D)\bigl(3\log(\psi(|D|)+1) + 2\psi(|D|)M(D) + B_\Phi(D)\bigr) \le B_\gamma(D). \tag{3.6}$$

A calculation completely analogous to that used in (3.5) yields

$$\log|2\beta_{0,2}(\alpha_Q) + \beta_{1,1}(\alpha_Q)| \le 3\log(\psi(|D|+1) + \mathrm{ht}(\phi) + \psi(|D|)M + 2, \tag{3.7}$$

for all $Q \in \mathcal{Q}_D^{\mathrm{prim}}$. The absolute values of the numerators of the coefficients of $H_D(\gamma; x)$, which has degree $h(D)$, have logarithms that exceed the bound in (3.7) by at most $\log 2^{h(D)}$. Combining this with (3.6) yields

$$\mathrm{ht}(\delta H_D(\gamma; x)) \le \log|\delta| + 3\log(\psi(|D|+1) + \mathrm{ht}(\phi) + \psi(|D|)M + + h(D)\log 2 + 2, \tag{3.8}$$

and it is then easy to check that plugging (3.4) and (3.6) into the RHS yields an expression that is bounded by $B_\gamma(D)$ as defined in (3.3). The asymptotic bound $B_\gamma(D) = \widetilde{O}(|D|^{3/2})$ follows immediately from the bounds $h(D) = \widetilde{O}(|D|^{1/2})$, $\psi(|D|) = \widetilde{O}(|D|)$, $M(D) = \widetilde{O}(|D|^{1/2})$ and $B_\Phi(D) = \widetilde{O}(|D|)$. □

For an odd prime ℓ, given a suitable order $\mathcal{O}$ and a suitable prime p, the isogeny volcano algorithm of [6, Alg. 2.1] computes Φ_ℓ in $\widetilde{O}(\ell^2)$ time, provided that $\log p = O(\log \ell)$. Here we extend this result to any integer $m > 1$. We first note that

$$\begin{aligned}\Phi_2(X,Y) =& X^3 + Y^3 - X^2Y^2 + 1488(X^2Y + XY^2) - 162000(X^2 + Y^2)\\ &+ 40773375XY + 8748000000(X+Y) - 157464000000000,\end{aligned}$$

and extend Definition 2.1 to composite integers m.

Definition 3.2. Let $m > 1$ be an integer, let ℓ be the largest prime divisor of m. An imaginary quadratic order $\mathcal{O}$ is said to be *suitable* for m if $\psi(m) + 1 \le h(\mathcal{O}) \le 3\psi(m)$ and $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$. A prime p is *suitable* for m and $\mathcal{O}$ if $p \equiv 1 \bmod \ell$ and $4p = t^2 - \ell^2 v^2 \operatorname{disc}(\mathcal{O})$ for some $t, v \in \mathbb{Z}$ with $\ell \nmid v$.

Algorithm 1.1
Input: An integer $m > 1$, an order $\mathcal{O}$ suitable for m, and a prime p suitable for m and $\mathcal{O}$.
Output: The modular polynomial $\Phi_m \bmod p$.

1. If $m = 2$ then output $\Phi_2 \bmod p$ and terminate.
2. If m is an odd prime then compute $\Phi_m \bmod p$ via [6, Alg. 2.1] and terminate.
3. Compute Φ_ℓ for each prime $\ell \le \sqrt{m}$ dividing m.
4. Compute the Hilbert class polynomial H_D, where $D = \operatorname{disc}(\mathcal{O})$, via [33, Alg 2].
5. Compute the roots $j_1, \dots, j_h \in \mathbb{F}_p$ of $H_D \bmod p$ and let $S = \{j_1, \dots, j_n\}$, where $n = \psi(m) + 1$.
6. If m has a prime divisor $\ell_0 > \sqrt{m}$ then compute n sets of j-invariants $S_1^0, \dots, S_n^0$, where $S_i^0 = \{\tilde{j} \in \mathbb{F}_p : \Phi_{\ell_0}(j_i, \tilde{j}) = 0\}$, using the isogeny volcano method.
   Otherwise, let $\ell_0 = 1$, and let $S_i^0 = \{j_i\}$ for $1 \le i \le n$.
7. Let $\ell_1 \le \ell_2 \le \cdots \le \ell_r$ be the primes whose product is m/ℓ_0.
   For $1 \le d \le r$ do the following:
   a. If $\ell_d \ne \ell_{d-1}$ then compute $S_i^d = \{\tilde{j} \in \mathbb{F}_p : \Phi_{\ell_i}(j_k, \tilde{j})$ for some $j_k \in S_i^{d-1}\}$ for $1 \le i \le n$.
   b. If $\ell_d = \ell_{d-1}$ then compute $S_i^d = \{\tilde{j} \in \mathbb{F}_p : \Phi_{\ell_i}(j_k, \tilde{j})$ for some $j_k \in S_i^{d-1} \backslash S_i^{d-2}\}$ for $1 \le i \le n$.
8. For $1 \le i \le n$ compute $\phi_i(X) = \Phi_m(X, j_i) = \sum_{k=0}^{\psi(m)} a_{ik} X^k$ as the product $\prod_{\tilde{j} \in S_i^r}(X - \tilde{j})$.
9. For $0 \le k \le n$ interpolate the polynomial $f_k(X)$ of degree less than n for which $f_k(j_i) = a_{ik}$.
10. Output $\Phi_m(X,Y) = \sum_{k=0}^{\psi(m)} f_k Y^k \bmod p$.

Note that step 6 does not use Φ_{ℓ_0} to compute S_i^0, it uses the isogeny volcano method detailed in [6, §6], whereas step 7 uses the (smaller) polynomials Φ_ℓ computed in step 3. When computing $\Phi_m \bmod p$ for many primes p (as in Algorithm 1), the polynomials $H_D \in \mathbb{Z}[x]$ and $\Phi_\ell \in \mathbb{Z}[X,Y]$ computed in steps 3 and 4 may be computed just once and reused, since they do not depend on p.

Lemma 3.3. *Algorithm 1.1 correctly computes $\Phi_m(X,Y) \bmod p$. Under the GRH, its expected running time is $\widetilde{O}(m^2)$, provided that $\log p = O(\log m)$.*

Proof. For each of the j-invariants $j_i \in S$, the set S_i^d contains all the j-invariants $\tilde{\jmath}$ for which $\Phi_{m_d}(j_i,\tilde{\jmath}) = 0$, where $m_d = \prod_{i=0}^{d} \ell_d$. This follows from the defining property of $\Phi_m(X,Y)$ (it parameterizes cyclic m-isogenies) and the fact that every (separable) cyclic isogeny can be expressed as a product of cyclic isogenies of prime degree (note that p is distinct from all the ℓ_i, since $p \equiv 1 \bmod \ell_i$). Thus we have $\phi_i(X) = \Phi_m(X, j_i)$ in step 8, and the $n = \psi(m) + 1$ distinct values of $j_i \in S$ are sufficient to uniquely determine the coefficients of $\Phi_m \bmod p$ in step 9.

We now bound the complexity of each step, assuming the GRH and that $\log p = O(\log m)$. Step 1 takes $\widetilde{O}(1)$ time and step 2 takes $\widetilde{O}(m^2)$ time, by [6, Thm. 6.5]. Computing $O(\log m)$ modular polynomials Φ_ℓ with $\ell \le \sqrt{m}$ in step 3 takes $\widetilde{O}(m^{3/2})$ expected time, by [6, Thm. 1]. We have $h = h(D) = O(m)$, since $\mathcal{O}$ is suitable for m, and since $h(D) = \widetilde{O}(|D|^{1/2})$, we have $|D| = \widetilde{O}(m^2)$ and this bounds the cost of step 3, by [33, Thm. 1]. Using standard probabilistic algorithms for root-finding, step 5 takes $\widetilde{O}(h)$ expected time, which is $\widetilde{O}(m)$.

The cost of step 6 is bounded by $\widetilde{O}(h\ell_0 + \ell_0^2)$, which is $\widetilde{O}(m^2)$; this follows from the proof of [6, Thm. 6.5]. Step 7 consists of root-finding operations in $\mathbb{F}_p$ whose expected complexity is softly-linear in the number of roots, ignoring factors of $\log p$ (every polynomial under consideration splits completely $\mathbb{F}_p[x]$ by virtue of the suitability of $\mathcal{O}$ and p). The total number of roots computed in step 7 is $O(\psi(m)^2)$, hence the total cost is $\widetilde{O}(m^2)$ expected time.

Using standard algorithms for fast arithmetic and polynomial interpolation [18], the cost of steps 8 and 9 are both bounded by $\widetilde{O}(\psi(m)^2)$, which is $\widetilde{O}(m^2)$. Thus every step has an expected running time bounded by $\widetilde{O}(m^2)$. □

Corollary 3.4. *Under the GRH, for any integer $m > 1$ the modular polynomial Φ_m can be computed in $\widetilde{O}(m^3)$ expected time.*

Proof. An explicit $\widetilde{O}(m)$ bound on the height of Φ_m can be derived from [9, Prop. 13.14] using the height bounds for Φ_ℓ for primes $\ell | m$ given in (2.5). An order $\mathcal{O}$ suitable for m can be obtained from the family of suitable orders given in [6, Ex. 4.3] and a sufficiently large set S of primes p suitable for m and $\mathcal{O}$ can be selected using [6, Alg. 6.2]. Under the GRH, these primes satisfy $\log p = O(\log m)$ and the corollary then follows from Lemma 3.3 and standard bounds on the time for fast Chinese remaindering [18, §10.3]. □

Remark. An algorithm to compute Φ_m using floating point approximations appears in [15] with a running time that is also $\tilde{O}(m^3)$, but the correctness of this algorithm and the bound on its running time both depend on a heuristic assumption regarding the precision needed to avoid rounding errors. We note that Algorithm 1.2 is faster in practice, its output is provably correct, and the bound on its expected running time depends only on the GRH.

Corollary 3.5. *Let D be an imaginary quadratic discriminant that is not special, let $\mathcal{O}$ be an order suitable for $|D|$ with $h(D) = O(|D|)$, and let p be a prime suitable for $|D|$ and $\mathcal{O}$. Under the GRH, the polynomial $H_D(\gamma; x) \bmod p$ can be computed in $\widetilde{O}(|D|^2)$ expected time.*

Proof. Apply Lemma 3.3 to step 3 of Algorithm 1. □

We now prove Theorem 1.1 given in the introduction, which we restate here.

Theorem 1.1. *Algorithm 1 computes $H_D(\gamma; x)$. Under the GRH, its expected running time is $\widetilde{O}(|D|^{7/2})$ and it uses $\widetilde{O}(|D|^2)$ space.*

Proof. The correctness of Algorithm 1 follows from the discussion preceding the algorithm, which shows how to compute $H_D(\gamma; x)$ in terms of Φ_D and the Hilbert class polynomial H_D, the correctness of the algorithm used to compute H_D [33, Thm. 1], the correctness of Algorithm 1.1 used to compute $\Phi_D \bmod p$ (Lemma 3.3), and the validity of the bound $B_\gamma(D)$ on the logarithmic height of $H_D(\gamma; x)$ (Lemma 3.1).

For the time and space bounds, we now assume the GRH. We first note that, as explained in §2.3, we can select the set of primes S in step 1 in $O(B_\gamma(D)^{1+\epsilon})$ time, which is $O(|D|^{3/2+\epsilon})$ for any $\epsilon > 0$, since $B_\gamma(D)$ is $\widetilde{O}(|D|^{3/2})$, by Lemma 3.1, and the primes $p \in S$ all satisfy $\log p = O(\log |D|)$. The time to compute the Hilbert class polynomial H_D in step 2 is $\widetilde{O}(|D|)$, by [33, Thm. 1], and its size is $\widetilde{O}(|D|)$. The set S has cardinality $O(B_\gamma(D))$, which is $\widetilde{O}(|D|^{3/2})$, and each iteration of step 3 takes $\widetilde{O}(|D|^2)$ expected time: this follows from Lemma 3.3, the time for fast multipoint polynomial evaluation [18, Cor. 10.8], and standard bounds on the complexity of fast arithmetic in $\mathbb{F}_p[x]$. Thus the total expected time for step 3 is $\widetilde{O}(|D|^{7/2})$.

The space used in each iteration of step 3 must be bounded by $\widetilde{O}(|D|^2)$, since this bounds the time, and the total size of the values $f(x) \bmod p$ and $\delta \bmod p$ saved is bounded by $O(h(D)B_\gamma(D))$, which is $\widetilde{O}(|D|^2)$. Finally, with fast Chinese remaindering [18, Alg. 10.22], the cost of step 4 is softly-linear in the total size of the coefficients of $\delta H_D(\gamma; x)$ and δ, which is $\widetilde{O}(|D|^2)$. □

3.2. **Algorithm 2.** We now give an algorithm to compute the class polynomial $H_D(F; x)$ for a good modular function $F(z) = \sum A_n(z)\gamma(z)^n$, as defined in the introduction. We assume that each $A_n(z)$ is written in the form $A_n(z) = r_n(j(z))$, where $r_n \in \mathbb{Z}(x)$.

Algorithm 2
Input: An imaginary quadratic discriminant D that is not special.
Output: The polynomial $H_D(F; x) \in \mathbb{Q}[x]$.

1. Pick an order $\mathcal{O}$ lying in the order of discriminant D that is also suitable for $|D|$, and a set S of primes suitable for $|D|$ and $\mathcal{O}$ (see Def. 3.2) such that no prime in S divides the denominator of any of the $r_n(x)$, using the height bound $B_F(D)$ (discussed below).
2. Compute the Hilbert class polynomial $H_D \in \mathbb{Z}[x]$ using [33, Alg. 2].
3. For each prime $p \in S$:
   a. Compute $\Phi_D \bmod p$ using Algorithm 1.1.
   b. Compute the roots $j_1, \dots, j_h \in \mathbb{F}_p$ of $H_D \bmod p$.
   c. For each j_k do the following:

i. Compute $\gamma_k = (2\beta_{0,2} - \beta_{1,1})/\beta_{0,1} \bmod p$ as in Algorithm 1.
ii. Compute $F_k = \sum r_n(j_k)\gamma_k^n \bmod p$.
d. Compute $f(x) = c_1|D|^{c_2 h} \prod_k (x - F_k) \bmod p$.
e. Save $f(x) \bmod p$.
4. Use the CRT to recover $f(x) = c_1|D|^{c_2 h(D)} H_D(F;x) \in \mathbb{Z}[x]$.
5. Output $H_D(F;x) = \frac{1}{c_1}|D|^{-c_2 h(D)} f(x) \in \mathbb{Q}[x]$.

The bound $B_F(D)$ used in step 1 is an upper bound on $\operatorname{ht}\left(c_1|D|^{c_2 h(D)} H_D(F;x)\right)$, which the next result shows is $\widetilde{O}(|D|^{1/2})$. Explicit computation of $B_F(D)$ depends on the particular functions $A_n(z)$; bounds on the heights of the class polynomials $H_D(A_n;x)$ can be readily derived from the functions $r_n(x)$ and known bounds on the height of the Hilbert class polynomial H_D; see Lemma 8 in [33], for example. From these, one can derive an explicit bound $B_F(D)$ on the height of $H_D(F;x)$; see Lemma 3.9 in the next section for an example. In general, the following lemma gives us an asymptotic bound for $B_F(D)$ that suffices to bound the complexity of Algorithm 2.

Lemma 3.6. *For all non-special imaginary quadratic discriminants D we have*

$$\operatorname{ht}\left(c_1|D|^{c_2 h(D)} H_D(F;x)\right) = \widetilde{O}(|D|^{1/2}).$$

Proof. The proof follows as in the proof of Lemma 8 of [33]. One only needs to take care of the dependence of the summand $\frac{3}{\pi \operatorname{Im}(z)}$ in the definition of $E_2^*(z)$ which in turn appears in the definition of $\gamma(z)$. We leave these details to the reader. □

We now prove Theorem 1.2 given in the introduction, which we restate here.

Theorem 1.2. *For discriminants $D < -4$ not of the form $D = -3d^2$, Algorithm 2 computes $H_D(F;x)$ for good modular functions $F(z)$. Under the GRH, its expected running time is $\widetilde{O}(|D|^{5/2})$ and it uses $\widetilde{O}(|D|^2)$ space.*

Proof. The correctness of Algorithm 2 is clear. We now bound its complexity, under the GRH. By Lemma 3.6, the set S contains $\widetilde{O}(|D|^{1/2})$ primes, and as described in §2.3, we can construct S in $\widetilde{O}(|D|^{1/2})$ expected time. The expected time to compute $H_D(X)$ in step 2 is $\widetilde{O}(|D|)$, by [33, Thm. 1]. Each of the primes $p \in S$ satisfies $\log p = O(\log |D|)$, and therefore the expected time for step 3a is $\widetilde{O}(|D|^2)$, by Lemma 3.3. This dominates the cost of steps 3b and 3c, and the total expected time for step 3 is thus $\widetilde{O}(|D|^{5/2})$, which dominates the expected running time of the entire algorithm. The space complexity of step 3 is dominated by the size of $\Phi_D \bmod p$, which is $\widetilde{O}(|D|^2)$. □

3.3. **Algorithm 3.** We now give an algorithm to compute the partition polynomial

$$H_n^{\text{part}}(x) := \prod_{Q \in \mathcal{Q}_{6,1-24n,1}} (x - P(\alpha_Q))$$

defined in (1.8). We do this by expressing $H_n^{\text{part}}(x)$ as a product of class polynomials

$$H_{D,\beta}(P;x) := \prod_{Q \in \mathcal{Q}_{6,D,\beta}^{\text{prim}}/\Gamma_0(6)} \left(x - P(\alpha_Q)\right). \tag{3.9}$$

Lemma 3.7. *For a positive integer n, let $D = 1 - 24n$. Then*

$$H_n^{\mathrm{part}}(x) = \prod_{\substack{u>0\\ u^2|D}} \varepsilon(u)^{h(D/u^2)} H_{D/u^2,1}(P; \varepsilon(u)x),$$

where the class polynomials on the right and side are defined by (3.9), and $\varepsilon(u) = 1$ if $u \equiv \pm 1 \bmod 12$ and $\varepsilon(u) = -1$ otherwise.

Proof. Using [20], p. 505 equation (1), we obtain

$$H_n^{\mathrm{part}}(x) = \prod_{\substack{u>0\\ u^2|1-24n}} H_{(1-24n)/u^2,\beta_u}(P; x), \tag{3.10}$$

where $\beta_u \in \mathbb{Z}/12\mathbb{Z}$ denotes the unique residue such that $\beta_u \cdot u \equiv 1 \pmod{12}$, equivalently, $\beta_u \equiv u \pmod{12}$.

Let $\Delta < 0$ be any discriminant such that $\Delta \equiv 1 \pmod{24}$. Since P is invariant under the Atkin-Lehner involution W_6, we have

$$H_{\Delta,-1}(P; x) = H_{\Delta,1}(P; x).$$

Since P is taken to its negative under the Atkin-Lehner involution W_3, we have

$$H_{\Delta,\pm 5}(P; x) = H_{\Delta,1}(-P; x) = (-1)^{h(\Delta)} H_{\Delta,1}(P; -x).$$

Putting this into (3.10), we obtain the assertion. □

For the remainder of this section (and also in Section 4), we shall abuse notation and drop the dependence on β for modular functions on $\Gamma_0(6)$. In every case we will have $\beta = 1$. For example, we let $H_D(P; x) := H_{D,1}(P; x)$ for convenience. We cannot directly apply Algorithm 2 to compute $H_D(P; x)$ because the function $P(z)$ does not satisfy all of our requirements for a good modular function; some minor changes are required, as we now explain.

As shown by Larson and Rolen, the function $P(z)$ may be decomposed as

$$P(z) = A(z) + B(z)\gamma(z), \tag{3.11}$$

where $\widehat{A}(z) = A(z)j(z)(j(z) - 1728)$ and $B(z)$ are weakly holomorphic modular functions for $\Gamma_0(6)$; see Lemma 2.2 in [26]. The expression for $P(z)$ in (3.11) does not satisfy our definition of a good modular function $F(z)$ because $A(z)$ and $B(z)$ are not rational functions of $j(z)$. However our two key requirements are satisfied: for discriminants D of the form $1 - 24n$, the values of $A(z)$ and $B(z)$ at CM points lie in the ring class field $K_{\mathcal{O}}$, and the polynomial $|D|H_D(P; x)$ has integer coefficients (so $c_1 = c_2 = 1$).

For each of the functions $g = \widehat{A}, B$, Larson and Rolen compute explicit polynomials

$$\Psi_g(X; z) := \prod_{\alpha} (X - g(\alpha z)),$$

where the product ranges over right coset representatives α for $\Gamma_0(6)$ in $\mathrm{SL}_2(\mathbb{Z})$. The polynomials Ψ_g may be expressed as polynomials in X whose coefficients are integer polynomials in $j(z)$, and we regard them as elements of $\mathbb{Z}[X, J]$; see Appendix A of [26] for the exact values of $\Psi_{\widehat{A}}$ and Ψ_B. Here each occurrence of $j(z)$ is replaced by the indeterminate J. While $\widehat{A}(z)$ and $B(z)$ are not rational functions of $j(z)$, we note that the curves defined by $\Psi_{\widehat{A}}(X, J)$ and

$\Psi_B(X,J)$ both have genus 0 (and thus admit a rational parametrization, although we shall not make explicit use of this fact).

It follows that, at least for discriminants prime to 6, the CM values of $\widehat{A}(z)$ and $B(z)$ are class invariants, and we can compute the class polynomials $H_D(\widehat{A};x)$ and $H_D(B;x)$ using standard algorithms such as those found in [5, 14, 16]. Under the GRH, we can compute these class polynomials in $\widetilde{O}(|D|)$ expected time, which is negligible compared to the $\widetilde{O}(|D|^{5/2})$ expected running time of Algorithm 2.

For $g = \widehat{A}, B$, we can use $H_D(g;x)$ to uniquely determine a root g_k of $\Psi_g(x,j_k)$ corresponding to a singular modulus j_k by computing the unique root of the linear polynomial

$$f_k(g;x) := \gcd\big(\Psi_g(x,j_k), H_D(g;x)\big).$$

This is useful because we would otherwise have 6 possible values of g_k to choose from; in both cases $\Psi_g(x,j_k)$ has degree 12, and 6 of its roots lie in the ring class field. In the context of Algorithm 2, we can use the values g_k to replace the quantities $r_n(j_k)$ in step 3.c.ii that require $A_n(z)$ to be a rational function of $j(z)$. For this purpose we let $\hat{a}_k$ and b_k denote the unique roots of the polynomials $f_k(\widehat{A};x)$ and $f_k(B;x)$, respectively, and let a_k denote $\hat{a}_k/(j_k(j_k-1728))$.

There is one other issue to consider. The coefficients of the class polynomials $H_D(\widehat{A};x)$ and $H_D(B;x)$ are not rational integers; they are algebraic integers in the quadratic field $K = \mathbb{Q}(\sqrt{D})$. This presents a potential difficulty for the CRT approach; while we always work modulo primes p for which D is a quadratic residue, we must make an arbitrary choice for the square root of D modulo p, and there is no clear way to make these choices consistently across many primes p. The following lemma implies that it does not matter which choice we make, we will get the same answer in either case.

Lemma 3.8. *Let $P(z) = \widehat{A}(z)/(j(z)(j(z)-1728)+B(z)\gamma(z)$ be as above. Then for any discriminant $D = 1-24n$, we have*

$$\{P(\alpha_Q) : \alpha_Q \in \mathcal{Q}^{\mathrm{prim}}_{6,D,\beta}/\Gamma_0(6)\} = \{\overline{P(\alpha_Q)} : \alpha_Q \in \mathcal{Q}^{\mathrm{prim}}_{6,D,\beta}/\Gamma_0(6)\}.$$

Proof. For any modular function f as P (e.g. any weak Maass form) with real coefficients, we have

$$\{(f \mid W_6)(\alpha_Q) : \alpha_Q \in \mathcal{Q}^{\mathrm{prim}}_{N,D,\beta}/\Gamma_0(6)\} = \{\overline{f(\alpha_Q)} : \alpha_Q \in \mathcal{Q}^{\mathrm{prim}}_{N,D,\beta}/\Gamma_0(6)\}.$$

Using the invariance of P under W_6, we get

$$\{P(\alpha_Q) : \alpha_Q \in \mathcal{Q}^{\mathrm{prim}}_{6,D,\beta}/\Gamma_0(6)\} = \{\overline{P(\alpha_Q)} : \alpha_Q \in \mathcal{Q}^{\mathrm{prim}}_{6,D,\beta}/\Gamma_0(6)\}.$$

□

We now give the algorithm to compute the partition polynomial $H_n^{\mathrm{part}}(x)$.

Algorithm 3
Input: A positive integer n.
Output: The partition polynomial $H_n^{\mathrm{part}}(x) \in \mathbb{Q}[x]$.

1. Let $1-24n = v^2 D_0$, where D_0 is a fundamental discriminant.
2. For each divisor u of v, let $D = u^2 D_0$ and compute $H_D(P;x)$ as follows:

a. Compute the class polynomials $H_D(\widehat{A};x)$ and $H_D(B;x)$.
b. Using the height bound $B_P(D)$ defined below, compute the polynomial $H_D(P;x)$ using a modified version of Algorithm 2 in which $r_0(j_k)$ is replaced by $a_k = \widehat{a}_k/(j_k(j_k-1728))$ and $r_1(j_k)$ is replaced by b_k, where a_k and b_k are as defined above.

3. Compute $H_n^{\mathrm{part}}(x) \in \mathbb{Q}[x]$ via Lemma 3.7.

The height bound $B_P(D)$ is defined as

$$B_P(D) := c_1 B_j(D) + h(D)\log|D|, \tag{3.12}$$

where $B_j(D)$ is an explicit bound on the height of the Hilbert class polynomial derived as in Lemma 8 of [33]. Here c_1 denotes an effectively computable positive constant.

Remark. We have not tried to obtain the optimal constant for c_1. However, it is reasonable to suspect that we can take $c_1 := 7/3$, which we note is equal to $\deg_J(\Psi_{\widehat{A}})/\deg_X(\Psi_{\widehat{A}}) = 28/12$ (which dominates $\deg_J(\Psi_B)/\deg_X(\Psi_B) = 18/12$).

Lemma 3.9. *For all discriminants $D \equiv 1 \bmod 24$ we have $\mathrm{ht}\big(H_D(P;x)\big) \le B_P(D)$.*

Proof. The proof is analogous to the proof of Lemma 3.6, which in turn follows as in the proof of Lemma 8 of [33]. Decorating that proof with the asymptotic properties of the Fourier expansion of the function $P(z)$, which is the image of a simple weight -2 weakly holomorphic modular form under the differential operator $\partial_{-2} := \frac{1}{2\pi i}\cdot\frac{\partial}{\partial z} + \frac{1}{2\pi \mathrm{Im}(z)}$, gives the desired result. □

We now prove Theorem 1.3 given in the introduction, which we restate here.

Theorem 1.3. *For all positive integers n, Algorithm 3 computes $H_n^{\mathrm{part}}(x)$. Under the GRH, its expected running time is $\widetilde{O}(n^{5/2})$ and it uses $\widetilde{O}(n^2)$ space.*

Proof. The correctness of Algorithm 3 follows from Lemmas 3.7 and 3.8, and the correctness of Algorithm 2. For the complexity bound, we first note that the degree of $H_n^{\mathrm{part}}(x)$ is given by the Hurwitz-Kronecker class number $H(1-24n) = \sum_D h(D)$, where D varies over negative discriminants dividing $1-24n$. It is known that $H(D) = O\big(h(D)(\log\log|D|)^2\big)$; see, e.g., [33, Lemma 9]. The complexity bounds then follow from the height bound in Lemma 3.9 and the complexity bounds in Theorem 1.2. □

To simplify the practical implementation of Algorithm 3, we make the following remark: it is not actually necessary to compute the class polynomials $H_D(\hat{A};x)$ and $H_D(B;x)$. Instead, for each singular modulus j_k, one can simply compute all 36 possible combinations $s_i + t_i j_k$, where $s_1,\dots,s_6$ are the roots of $\Psi_{\hat{A}}(x,j_k)$ that lie in $\mathbb{F}_p$ (where $p \equiv 11 \bmod 12$ is a suitable prime) and $t_1,\dots,t_6$ are the roots of $\Psi_B(x,j_k)$ that lie in $\mathbb{F}_p$. For all but finitely many primes p, exactly 32 of these 36 values will be distinct, and there will be two pairs of repeated values, corresponding to $P_k = a_k + b_k j_k$ and $-P_k = -a_k - b_k j_k$. We do not prove this claim here, but observe that Lemma 3.8 guarantees that the value P_k will be repeated, so if one in fact finds the situation modulo p to be as claimed (exactly two pairs of repeated values that differ only in sign), then the end result will be provably correct. For the handful of primes p where the claim does not hold, one simply discards p and selects another suitable prime in its place.

Using the observation above, one may compute the polynomial

$$f(x) = |D|^{2h(D)} \prod_k (x^2 - P_k^2) = (-1)^{h(D)} |D|^{2h(D)} H_D(P;x) H_D(P;-x) \bmod p$$

modulo a sufficient number of primes p (using a suitably increased height bound), and then apply the CRT to obtain the integer polynomial $f(x)$ which may then be factored in $\mathbb{Z}[x]$ to yield the required polynomial $H_D(P;x)$.

4. Numerical examples

As a first example, let us compute $H_1^{\mathrm{part}}(x)$ using Algorithm 3, recapitulating the example given in the introduction of [8]. We have $n = 1$, and the discriminant $D = 1 - 24n = -23$ is fundamental, so $u = 1$. We begin by computing the class polynomials

$$\begin{aligned} H_{-23}(\widehat{A};x) &= x^3 + (264101659831625\Delta - 76898070951625)/2\, x^2 \\ &\quad + (4866595720359935196250\Delta + 123772870000262550375 0)\, x \\ &\quad + (-1404875488681363726279402992 1875\Delta - 3105601444479222141757418176 5625)/2, \\ H_{-23}(B;x) &= x^3 + (-35487375\Delta - 35487375)\, x^2 + (6837889760625\Delta - 75216787366875)/2\, x \\ &\quad + (842331597312734375\Delta + 2863927430863296875)/2, \end{aligned}$$

where Δ denotes a square root of -23. We then compute the *heuristic* height bound

$$B_P(-23) = 7/3\ B_j(-23) + h(-23)\log 23 \approx 83.25$$

for $H_{-23}(P;x)$, using [33, Lemma 8] to compute $B_j(-23) \approx 31.65$.

Remark. We refer to this bound as a heuristic bound because we used $c_1 = 7/3$ as in the discussion in the previous section. Implementing the algorithm with this bound for $n \le 750$ always gave the correct values for $p(n)$. Moreover, in every case the polynomials $H_D(P;x)$ computed by the algorithm split into linear factors over the ring class field for the order for discriminant D.

We now use Algorithm 2 to compute $H_{-23}(P;x)$, with $r_0(j_k) = \widehat{a}_k/(j_k(j_k - 1728))$ and $r_1(j_k) = b_k$. The order $\mathcal{O}$ of index 11 in the order of discriminant -23 is suitable for the integer 23, and the primes in the set

$$S = \{1562207, 2744591, 4294607, 6454031, 7089107, 10010291\}$$

are all suitable for $\mathcal{O}$ and 23, with $\prod_{p\in S} \log p \approx 91.93 > B_P(-23) + \log 2$. We then compute

$$H_{-23}(j;x) = x^3 + 3491750x^2 - 5151296875x + 12771880859375$$

using [33, Alg. 2].

Starting with the first prime $p = 1562207$, we compute $\Phi_{23} \bmod p$ using Algorithm 1.1 (which in this case just calls [6, Alg. 2.1], since 23 is prime). We then find the roots j_k of $H_{-23}(x) \bmod p$, and for each j_k we compute:

- $\gamma_k = (2\beta_{0,2} - \beta_{1,1})/\beta_{0,1} \bmod p$ (via (2.9), using $\Phi_{23} \bmod p$ and j_k).
- $\widehat{a}_k$ as the unique root of $f_k(\hat{A};x) = \gcd\big(H_{-23}(\hat{A};x), \Psi_{\widehat{A}}(x,j_k)\big) \bmod p$.
- b_k as the unique root of $f_k(B;x) = \gcd\big(H_{-23}(B;x), \Psi_B(x,j_k)\big) \bmod p$.
- $P_k = a_k/(j_k(1728 - j_k)) + b_k\gamma_k$.

For the prime $p = 1562207$ the results of these computations are summarized below.

	$k=1$	$k=2$	$k=3$
j_k:	244476	467416	482979
γ_k:	1461486	587848	220836
$\widehat{a}_k$:	1201792	98544	239915
b_k:	1120135	560362	531933
P_k:	1352290	519913	1252234

Using the constants $c_1 = c_2 = 1$ in our definition of a good modular function, we compute

$$f(x) = 23^3 \prod_k (x - P_k) = 12167x^3 + 1282366x^2 + 337961x + 1150855 \pmod{1562207}$$

as the reduction of $|D|^{h(D)} H_D(P; x)$ modulo p. Repeating this process for the remaining primes in S yields the following polynomials $|D|^{h(D)} H_D(P; x)$ mod p.

$$\begin{aligned}
&12167x^3 + 2464750x^2 + 1900168x + 391209 \pmod{2744591}\\
&12167x^3 + 4014766x^2 + 1900168x + 3491241 \pmod{4294607}\\
&12167x^3 + 6174190x^2 + 1900168x + 1356058 \pmod{6454031}\\
&12167x^3 + 6809266x^2 + 1900168x + 1991134 \pmod{7089107}\\
&12167x^3 + 9730450x^2 + 1900168x + 4912318 \pmod{1001029}
\end{aligned}$$

Applying the Chinese remainder theorem, and using the fact that $\prod_{p\in S} p$ is more than twice the absolute value of the largest coefficient of $23^3 H_{-23}(P; x)$, we obtain

$$23^3 H_{-23}(P; x) = 12167x^3 - 279841x^2 + 1900168x - 5097973 \in \mathbb{Z}[x].$$

We note that the coefficients of the above polynomial are all much smaller than the product

$$\prod_{p\in S} p = 539846566693883065928341753589603 9,$$

indicating that our height bound $B_P(-23)$ is actually bigger than it needs to be. Dividing by 23^3 and applying Lemma 3.7 we obtain

$$H_1^{\mathrm{part}}(x) = H_{-23}(P; x) = x^3 - 23x^2 + \frac{3592}{23}x - 419,$$

which completes the execution of Algorithm 3 for $n = 1$. As proven in [8], if we divide the trace of $H_n^{\mathrm{part}}(x)$ by $24n - 1$, we obtain the nth partition number $p(n)$. In this case we have $23/23 = 1 = p(1)$.

We now consider the case $n = 24$, which is the least n for which $1-24n$ is not a fundamental discriminant. We have $1 - 24 \cdot 24 = -575 = -5^2 \cdot 23$, and Lemma 3.7 then implies that

$$H_{24}^{\mathrm{part}}(x) = -H_{-23}(P; -x) H_{-575}(P; x). \tag{4.1}$$

We have already computed $H_{-23}(P;x)$, and in the same way we may compute

$$\begin{aligned}H_{-575}(P;x) = x^{18} &- 905648\,x^{17} + 7864919720287/23\,x^{16} - 62085428963462224\,x^{15}\\ &+ 250081922080066329031003 1/529\,x^{14} - 14557036936813234587879395 1/23\,x^{13}\\ &\cdots\\ &+ 75800599730923914197928048072994405278947818218326795 2/3700897225\,x\\ &- 27498975581954522601938667194305699500386654372043941 9/18504486125.\end{aligned}$$

From (4.1) we obtain

$$\begin{aligned}H_{24}^{\mathrm{part}}(x) = x^{21} &- 905625\,x^{20} + 341932201569\,x^{19} - 62077564185180110\,x^{18}\\ &+ 250006385563705574291667 9/529\,x^{17} - 14306977315489711798199227 5/23\,x^{16}\\ &- 24868250807372459203418508369590 4/60835\,x^{15}\\ &+ 47212745132954796287530489466980 42/2645\,x^{14}\\ &- 68424086670175524844820541966001817814 7/1399205\,x^{13}\\ &+ 82829752509115391200118877248705539565 6/12167\,x^{12}\\ &- 32704304695374273471069347508729088366971453/6436343\,x^{11}\\ &+ 29055302884240205748172908066542287477130660 1/1399205\,x^{10}\\ &- 15618334996574598433984982031615985504271825288372/3700897225\,x^{9}\\ &+ 29711382612712898396509661429593765717884169527 12/160908575\,x^{8}\\ &+ 67822191247241980381807708488720865403444300542792174/85120636175\,x^{7}\\ &- 10287891953477631667871642653944942982233172929865507/740179445\,x^{6}\\ &+ 12007217296006782069511589291297629940381387819392350475 8/1957774632025\,x^{5}\\ &+ 94421553321458076136220102025268816685173307920461335 29/17024127235\,x^{4}\\ &- 94456653168975353200367637648753191550199027182518415685547 7/225144082682875\,x^{3}\\ &- 51251514650146719914076454215115041896327911830821351834671 7/9788873160125\,x^{2}\\ &- 35536755774418816044099930383528934576071175834569478740 72/425603180875\,x\\ &+ 11522070768838944970212301554414088090662008181886411656 1/18504486125.\end{aligned}$$

If we divide the trace 905625 of $H_{24}^{\mathrm{part}}(x)$ by $24\cdot 24-1=575$ we obtain the partition number $p(24)=1575$, as expected. A table of all the polynomials $H_n^{\mathrm{part}}(x)$ for $n\le 750$ is available online at http://math.mit.edu/~drew.

References

[1] J. Belding, R. Bröker, A. Enge, and K. Lauter, *Computing Hilbert class polynomials*, Algorithmic Number Theory 8th International Symposium (ANTS VIII), eds. A. J. van der Poorten and A. Stein, LNCS **5011**, Springer, 2008, 282–295.

[2] W. E. H. Berwick, *Modular invariants*, Proc. London Math. Soc. **28** (1927), 53–69.

[3] A. Borel, S. Chowla, C. S. Herz, K. Iwasawa, and J.-P. Serre, *Seminar on complex multiplication*, Springer Lect. Notes. **21**, Springer Verlag, Berlin, 1966.

[4] K. Bringmann and K. Ono, *An arithmetic formula for the partition function*, Proc. Amer. Math. Soc. **135** (2007), 3507–3514.

[5] R. Bröker, *p-adic class invariants*, LMS J. Comput. Math. **14** (2011), 108–126.

[6] R. Bröker, K. Lauter, and A. V. Sutherland, *Modular polynomials via isogeny volcanoes*, Math. Comp. **81** (2012), 1201–1231.
[7] R. Bröker and A. V. Sutherland, *An explicit height bound for the classical modular polynomial*, Ramanujan Journal **22** (2010), 293–313.
[8] J. H. Bruinier and K. Ono, *Algebraic formulas for the coefficients of half-integral weight harmonic weak Maass forms*, preprint at http://arxiv.org/abs/1104.1182.
[9] D. A. Cox, *Primes of the form $x^2 + ny^2$*, Wiley and Sons, New York, 1989.
[10] M. Deuring *Die Klassenkörper der komplexen Multiplikation*, Enzyklopädie der mathematischen, Band I 2, Heft 10, Teil II, Teubner, Stuttgart (1958), 10–68.
[11] M. Deuring *Teilbarkeitseigenschaften der singulären Moduln der elliptischen Funktionen und die Diskriminante der Klassengleichung*, Comm. Math. Helv. **19** (1946), 74–82.
[12] D. Dorman, *Singular moduli, modular polynomials, and the index of the closure of $\mathbb{Z}[j(\tau)]$*, Math. Ann. **283** (1989), 177–191.
[13] D. Dorman, *Special values of the elliptic modular function and factorization formulae*, J. Reine Angew. Math. **383** (1988), 207–220.
[14] A. Enge, *The complexity of class polynomial computation via floating point approximations*, Math. Comp. **78** (2009), 1089–1107.
[15] A. Enge, *Computing modular polynomials in quasi-linear time*, Math. Comp. **78** (2009), 1809–1824.
[16] A. Enge and A. V. Sutherland, *Class invariants by the CRT method*, Algorithmic Number Theory 9th International Symposium (ANTS IX), eds. G. Hanrot, F. Morain, and E. Thomé, LNCS **6197**, Springer, 2010, 142–156.
[17] M. Fouquet and F. Morain, *Isogeny volcanoes and the SEA algorithm*, Algorithmic Number Theory 5th International Symposium (ANTS V), eds. C. Fieker and D. R. Kohel, LNCS **2369**, Springer, 2002, 276–291.
[18] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, second edition, Cambridge University Press, 2003.
[19] *B. Gross*, Heegner points on $X_0(N)$. Modular forms (Durham, 1983), 87–105, Horwood, Chichester (1984).
[20] B. Gross, W. Kohnen, and D. Zagier, *Heegner points and derivatives of L-series. II.* Math. Ann. **278** (1987), 497–562.
[21] B. Gross and D. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191-220.
[22] G. H. Hardy and S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. (2) **17** (1918), 75–115.
[23] F. Johansson, *Efficient implementation of the Hardy-Ramanujan-Rademacher formula*, LMS Journal of Computation and Mathematics **15** (2012), 341–359.
[24] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, PhD thesis, University of California at Berkeley, 1996.
[25] Serge Lang, *Elliptic functions*, second ed., Graduate Texts in Mathematics **112**, Springer-Verlag, 1987.
[26] E. Larson and L. Rolen, Integrality properties of the CM values of certain weak Maass forms, Algebra and Number Th., accepted for publication.
[27] David Masser, *Elliptic functions and transcendence*, Lecture Notes in Mathematics **437**, Springer, 1975.
[28] H. Rademacher, *On the partition function $p(n)$*, Proc. London Math. Soc. (2) **43** (1937), 241–254.
[29] H. Rademacher, *On the expansion of the partition function in a series*, Ann. Math. **44** (1943), 416–422.
[30] J.-P. Serre, *Complex Multiplication*, Algebraic Number Theory (J.W.S. Cassels and A. Fröhlich, eds.), Academic Press, 1967, 292–296.
[31] G. Shimura, *Arithmeticity in the theory of automorphic forms*, Amer. Math. Soc., 2000, Providence, RI.
[32] P. Solé and M. Planat, *Extreme values of the Dedekind ψ-function*, Journal of Combinatorics and Number Theory **3** (2011), 33–38.

[33] A. V. Sutherland, *Computing Hilbert class polynomials with the Chinese Remainder Theorem*, Math. Comp. **80** (2011), 501–538.
[34] A. V. Sutherland, *Isogeny volcanoes*, Algorithmic Number Theory 10th International Symposium (ANTS X), to appear, preprint at http://arxiv.org/abs/1208.5370.
[35] H. Weber, *Lehrbuch der Algebra*, Vol. III, 2nd edition, Chelsea, New York, 1961.
[36] D. Zagier, *Traces of singular moduli*, Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998) (2002), Int. Press Lect. Ser., 3, I, Int. Press, Somerville, MA, 211–244.

Fachbereich Mathematik, Technische Universität Darmstadt, Schlossgartenstrasse 7, D-64289, Darmstadt, Germany
E-mail address: bruinier@mathematik.tu-darmstadt.de

Department of Mathematics and Computer Science, Emory University, Atlanta, GA 30322
E-mail address: ono@mathcs.emory.edu

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139
E-mail address: drew@math.mit.edu